



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

mw

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/779,759

02/18/2004

Markus Miettinen

60279.00082

9776

32294

7590

08/24/2006

SQUIRE, SANDERS & DEMPSEY L.L.P.

14TH FLOOR

8000 TOWERS CRESCENT

TYSONS CORNER, VA 22182

EXAMINER

KIM, PAUL

ART UNIT

PAPER NUMBER

2161

DATE MAILED: 08/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/779,759

Applicant(s)

MIETTINEN ET AL.

Examiner

Paul Kim

Art Unit

2161

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 18 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.



**SAM RIMELL**  
**PRIMARY EXAMINER**

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This Office Action is responsive to the following communication: Original Application filed on 18 February 2004.

2. Claims 1-30 are pending and present for examination. Claims 1, 8, 15, 17, and 24 are independent.

#### *Priority*

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

#### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1, 5-6, 8, 12, 13, 15, 17, 21, 22, 24, 28, and 29** are rejected under 35 U.S.C. 102(e) as being anticipated by Belcaid et al (USPGPUB 2003/0065685, hereinafter referred to as BELCAID), filed on 24 July 2002, and published on 3 April 2003.

6. **As per independent claims 1 and 17**, BELCAID teaches:

A method for storing data records on a database system in which a signing entity is used for signing data records, the method comprising:

receiving a second data record to be stored on a database {See BELCAID, Para. 0025, wherein this reads over "slave database then retrieves, in step 202, the corresponding data A' from its memory"};

Art Unit: 2161

retrieving a first integrity checksum stored with a first data record previous to the second data record {See BELCAID, Para. 0025, wherein this reads over "the checksum C of data A from the master database"};

computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record {See BELCAID, Para. 0025, wherein this reads over "[t]he slave database then . . . calculates, in step 203, (using the same rules as the master database) a checksum C' for the corresponding data A'"}; and

storing the second data record and the second integrity checksum on the database {See BELCAID, Para. 0032, wherein this reads over "the master database starts to update the indicated data elements to the slave database"}.

**7. As per dependent claims 5, 12, 21, and 28, BELCAID teaches:**

The method according to claim 1, wherein the first integrity checksum is retrieved from a memory of a signing entity {See BELCAID, Para. 0025, wherein this reads over "the checksum C of data A from the master database"}.

**8. As per dependent claims 6, 13, 22, and 29, BELCAID teaches:**

The method according to claim 1, wherein the second integrity checksum is stored on a memory of the signing entity {See BELCAID, Para. 0018, wherein this reads over "each database can simultaneously be a master of some specific data and a slave of some other data"; and Para. 0025, wherein this reads over "[t]he slave database then . . . calculates, in step 203, (using the same rules as the master database) a checksum C' for the corresponding data A'"}.

**9. As per independent claims 8, 15, and 24, BELCAID teaches:**

A method for verifying integrity of data records on a database in which a verification entity is used for verifying integrity of data records, the method comprising:

retrieving a second data record to be verified from a first database {See BELCAID, Para. 0025, wherein this reads over "slave database then retrieves, in step 202, the corresponding data A' from its memory"};

retrieving a second integrity checksum of the second data record {See BELCAID, Para. 0027, wherein this reads over "the slave database retrieves, in step 209, the time stamp and the checksum of the corresponding data element from its memory"};

retrieving a first integrity checksum of a first data record previous to the retrieved second data record {See BELCAID, Para. 0025, wherein this reads over "the checksum C of data A from the master database"};

computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key {See BELCAID, Para. 0025, wherein this reads over "[t]he slave database then . . . calculates, in step 203, (using the same rules as the master database) a checksum C' for the corresponding data A'"}; and

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic if the second integrity checksum

Art Unit: 2161

and the third integrity checksums are equal {See BELCAID, Paras. 0025-0026, wherein this reads over "the slave database compares, in step 204, these two checksums C and C'. If they are the same, the slave database sends, in step 205, an acknowledgement 'ack' to the mast database indicating that no updating is necessary"}.

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. **Claims 2, 9, 16, 18, and 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over BELCAID, in view of Brown et al (USPGPUB 2003/0023850, hereinafter referred to as BROWN), filed on 26 July 2001, and published on 30 January 2003.

12. **As per dependent claims 2 and 18**, BELCAID, in combination with BROWN, discloses:

The method according to claim 1, wherein the storage key is a secret key of public key infrastructure {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session."}

The combination of inventions disclosed in BELCAID and BROWN would disclose a method wherein the storage key is a secret key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BELCAID by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

13. **As per dependent claims 9 and 25**, BELCAID, in combination with BROWN, discloses:

Art Unit: 2161

The method according to claim 8, wherein the storage key is a public key of public key infrastructure {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session"}.

The combination of inventions disclosed in BELCAID and BROWN would disclose a method wherein the storage key is a public key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BELCAID by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

14. **As per dependent claim 16**, BELCAID, in combination with BROWN, discloses:

The system according to claim 15, wherein the signing entity and verification entity apply public key infrastructure for calculating and verifying the one of the first integrity checksum and the second integrity checksum {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session."}.

The combination of inventions disclosed in BELCAID and BROWN would disclose a method wherein the public key infrastructure is applied for verification purposes. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BELCAID by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that either the first or second integrity checksum of the signing entity may be verified.

Art Unit: 2161

15. **Claims 3, 10, 19, and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over BELCAID, in view of Pond et al (U.S. Patent No. 4,864,616, hereinafter referred to as POND), filed on 15 October 1987, and issued on 5 September 5, 1989.

16. **As per dependent claims 3, 10, 19, and 26**, BELCAID, in combination with POND, discloses:

The method according to claim 1, wherein the retrieved integrity checksum for a first row of the database is a generated initialization vector {See POND, C3:L53-62, wherein this reads over "[t]he initialization vector contains bits for indicating the starting byte in each of the key streams used for encryption and decryption. The Checksum is derived by summing the . . . the Initialization Vector and issued to confirm the integrity of the label"}.

The combination of inventions disclosed in BELCAID and POND would disclose a method wherein the integrity checksum for a first row of a database is a generated initialization vector. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BELCAID by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that where there is no previous integrity checksum available, the initialization vector may be used to in the computation of a second integrity checksum.

17. **Claims 4, 11, 20, and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over BELCAID, in view of Applicant's Admitted Prior Art (hereinafter referred to as AAPA).

18. **As per dependent claims 4, 11, 20, and 27**, BELCAID, in combination with AAPA, discloses:

The method according to claim 1, wherein the retrieved integrity checksum for a first row of the database is a digital signature of the signing entity {See AAPA, Para. 0004, wherein this reads over "[w]ell-known methods for ensuring the integrity of a log file exist already today. . . [such as] digital signatures [which] can be used to associate a cryptographical code with each log"}.

19. **Claims 7, 14, 23, and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over BELCAID, in view of Cain (U.S. Patent No. 6,557,044, hereinafter referred to as CAIN), filed on 1 June 1999, and issued on 29 April 2003.

20. **As per dependent claims 7, 14, 23, and 30**, BELCAID, in combination with CAIN, discloses:

The method according to claim 1, wherein the integrity checksums comprise a running sequence number {See CAIN, c2:l64-67, wherein this reads over "incremental checksumming may be

Art Unit: 2161

utilized. Initially, the checksum for all routes in a set is computed by determining the checksum for all sequence numbers"}.


***Conclusion***

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Christian Chase can be reached on (571) 272-4190. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Paul Kim  
Patent Examiner, Art Unit 2161  
Technology Center 2100

  
**SAM RIMELL**  
**PRIMARY EXAMINER**